Gabriel S. Gross
Direct Dial: +1.650.463.2628
gabe.gross@lw.com

140 Scott Drive
Menlo Park, California 94025
Tel: +1.650.328.4600 Fax: +1.650.463.2600
www.lw.com

LATHAM & WATKINS LLP

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Shanghai
Hong Kong	Silicon Valley
Houston	Singapore
London	Tel Aviv
Los Angeles	Tokyo
Madrid	Washington, D.C.

File No. 072290-0003

August 10, 2022

Hon. Jeremiah J. McCarthy
United States District Court
Western District of New York
Robert H. Jackson United States Courthouse
2 Niagara Square
Buffalo, New York 14202

Re: *Moog Inc. v. Skyryse, Inc. et al.*, Case No. 1:22-cv-00187

Dear Magistrate Judge McCarthy:

Pursuant to the Court's order (ECF 206), Skyryse submits this letter in response to Moog's August 3, 2022 supplemental letter brief (ECF 211).

The iDS Protocol (1) lacks critical security measures necessary to safeguard a single party's proprietary, confidential source code in discovery, and (2) the complicated process it imposes—including forcing the parties to turn over their files to a third party—was never intended to govern the inspection of one side's materials that do *not* contain a combination of both sides' information. (*See* IDS Protocol, ECF 96-2; *see also* Motion, ECF 213.) Conversely, Skyryse's proposed source code protocol, which closely follows standard source code protocols implemented by courts across the country, provides these critical security measures and will benefit both sides when they make their source code available for inspection. (ECF 213-2.)

After no doubt scouring dockets across the country in search of other protective orders that Moog could argue support its position, Moog in its supplemental briefing has identified only four cases. They do not help Moog; not one is from a trade secret case that suggests source code should be provided to a neutral third party for purposes of allowing side-by-side comparisons, as Moog proposes here. Instead, Moog cites primarily to inapplicable *copyright* cases and cases that involve producing code directly to the opposing party, not to a third party.

Rather, the great weight of authority across the country makes clear that source code inspections in trade secret cases should be handled in the manner that Skyryse has proposed, allowing full inspections with thoughtful security restrictions. (ECF 213-2.) *See, e.g.*, *Virgilant Techs. Ltd. v. ABC Assets, Inc.*, 1:21-cv-00181-MN, Dkt. #61 (D. Del. June 23, 2022) (entering protective order in a trade secret case providing for stand-alone review of computers that "shall not be connected to the Internet or any other network while in the source code review room" whereby "[t]he stand-alone computer shall be located at the offices of the producing party's

Delaware outside counsel");[1] *see also Hullinger v. Anand*, 2:15-cv-07185-SJO-FFM, Dkt. #238 (C.D. Cal. June 30, 2016); *Lithero, LLC v. AstraZeneca Pharm. LP*, 1:19-cv-02320-RGA, Dkt. #93 (D. Del. Feb. 22, 2021); *ResMan, LLC v. Karya Prop. Mgmt, LLC*, 4:19-cv-00402-ALM, Dkt. #24 (E.D. Tex. June 17, 2019); *Carolina Coupon Clearing, Inc. v. Cardinal Health Managed Care Servs.*, LLC, 1:16-cv-00412-WO-JEP, Dkt. #163 (M.D.N.C. Feb. 16, 2017); *Level One Techs., Inc. v. Penske Truck Leasing Co., L.P.*, 4:14-cv-01305-ROW, Dkt. #57 (E.D. Mo. Feb. 23, 2016); *T.N. Inc. Ltd. v. Fidelity Nat'l Info. Servs., Inc.*, 2:18-cv-05552-WB, Dkt. #85 (E.D. Pa. Sept. 4, 2020); *Crowdstrike, Inc. v. NSS Labs, Inc.*, 1:17-cv-00146-MN, Dkt. #53 (D. Del. Apr. 3, 2018). Each of the foregoing protective orders,[2] entered in trade secret cases requiring source code productions, closely follow Skyryse's proposed source code protocol.

1. Moog's "side-by-side" argument is flawed.

Moog does not deny that Skyryse's proposal will allow the parties to fully inspect each other's highly confidential source code, or that it would do so in a secure manner. Instead, Moog argues that the Court should reject Skyryse's protocol because it takes an approach commonly used in patent infringement cases, while this is a trade secret case.[3] (ECF 211 at 3.) Specifically, Moog complains that it could not run automated "side-by-side" comparisons of the code under Skyryse's proposal. According to Moog, the relevant inquiry in a patent case is how a defendant's allegedly infringing source code compares *to a plaintiff's patent claims*, not to the plaintiff's source code, so side-by-side comparisons of the parties' source code are unnecessary in those cases. What Moog fails to appreciate is that this same logic applies to trade secret cases like this one. In a trade secret case, one relevant inquiry is whether and how a defendant's allegedly misappropriated source code compares *to a plaintiff's trade secrets*, not to the plaintiff's source code as a whole.[4] As in patent cases, where the parties' discoverable source code typically contains countless unpatented features, so too in trade secret cases, the parties' discoverable source code typically contains countless non-secret features.

Allowing the parties to inspect their adversary's source code in discovery, to explore issues relevant to claims of patent infringement or trade secret misappropriation (and related defenses) makes sense. But letting them run automated comparisons of their *entire* discoverable codebases,

---

[1] Each of the additional protective orders cited above likewise were entered by courts in trade secret cases requiring source code was to be made available on standalone computers without access to the Internet or the opposing party's source code at the office of the producing party's counsel.

[2] The cited protective orders are all attached hereto for reference as Exhibit A.

[3] Moog conveniently ignores that this same approach is frequently used in trade secret cases too.

[4] *See, e.g.,* Ex. B (*Proofpoint, Inc. v. Vade Secure, Inc.*, C.A. No. 19-cv-04238-MMC, Final Verdict Form, Dkt. #795 (N.D. Cal. Aug. 20, 2021)). In *Proofpoint*, a trade secret case that similarly involved the alleged theft of source code, the jury was asked to determine misappropriation by comparing a few dozen alleged trade secrets to defendants' technology as implemented in the defendants' source code. *Id.* The analysis did not require a side-by-side comparison of plaintiffs' entire source code base against defendants' entire source code base.

hunting for any perceived similarities—even if they have nothing to do with a plaintiff's allegedly patented inventions or protectable trade secrets—makes no sense. Worse, it would encourage fishing expeditions, unnecessarily drive burden and expense, and incentivize "shoot first, aim later" tactics, where a plaintiff only articulates and discloses its alleged trade secrets *after* gaining access to its adversary's innovations for which it wants to try to take credit.

That risk is only more pronounced here, where (1) there is no indication that the Skyryse source code at issue contains *any* Moog information (for the Court already ordered the parties to turn over to iDS any such code that may contain both sides' information); (2) Skyryse's code has been available to Moog to inspect for weeks, yet Moog refuses to look at it unless it gets its way and is allowed to run automated side-by-side comparisons; and (3) Moog still has not disclosed to the Defendants a single one of its alleged trade secrets, despite telling the Court it has known how to identify more than one hundred thousand of them, including by file type and location, for months. (July 21, 2022 Tr., Dkt. #204, at 19:14-20:2.)

It is no coincidence that the few cases Moog found where side-by-side comparisons of source code were allowed are copyright cases, because the legal standard for copyright infringement—unlike in patent and trade secret cases—actually requires a finding of "substantial similarity." *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co. Inc.*, 499 U.S. 340, 361 (1991). For example, the protective order in the *AMO* case that Moog relies on comes from a copyright case, not a trade secret case. *AMO Dev., LLC v. Alcon LenSx, Inc.*, C.A. No. 20-842 (D. Del.). There, the infringement analysis required a side-by-side comparison of each and every line of plaintiffs' copyrighted source code against defendants' source code. This is not surprising, because copyright protects the expression of an idea, and not the idea itself.

The same is not true for trade secret claims; mere "similarity" is not the test. Moog first will have to establish its alleged trade secrets are, in fact, not generally known to or readily ascertainable by others, that they are the subject of reasonable measures to keep them a secret, and that they derive independent value from their secrecy, and *then* Moog will need to establish that Skyryse misappropriated them. 18 U.S.C. §§ 1839(3), (5). As the Court has repeatedly recognized, Moog will not and cannot possibly present to the Court or the jury 1.4 million, 136,000, or any other inordinate number of alleged trade secrets that meet these requirements. Instead, Moog will need to provide a specific, narrow set of trade secrets that the fact-finder will consider and compare to Skyryse's technology, possibly including its source code. No side-by-side comparisons of the parties' source code will be necessary, much less of their entire discoverable codebases. And as the Court already has ordered, Moog must provide a *narrative* response to Skyryse's Interrogatory No. 1, in which Moog will identify all of its allegedly misappropriated trade secrets. Under Skyryse's proposal, nothing prevents Moog's counsel or its experts from bringing that detailed description of Moog's alleged trade secrets along to an inspection of Skyryse's code, and comparing the two in depth.

2. Moog already has all the "side-by-side" capabilities it arguably could need.

As Moog admits, it has already had the opportunity to compare side-by-side Moog documents and source code to the devices and repositories Skyryse has already turned over to iDS, which even arguably contain some combination of *both* sides' information. There is no dispute

that for each of these devices and repositories, Moog already has the ability to compare the devices and repositories side-by-side with any other device or repository that was legitimately put in iDS's custody. Moog fails to present a viable argument why it needs more than this by further comparing Skyryse's proprietary source code side-by-side with its own source code.

Moog instead attempts to shoehorn routine inspections of each side's proprietary source code into the unique iDS Protocol that was only ever intended to handle discovery of forensic images containing a mix of Moog and Skyryse information. Despite radically different confidentiality concerns between the forensic images that were intended to go to iDS and each party's own proprietary source code, Moog seeks a "one size fits all" protocol, the iDS Protocol, because it claims there is no need for "a brand new inspection protocol" to address the unique concerns of proprietary source code. (ECF 211 at 6.) But, as demonstrated by the *Brocade* case relied upon by Moog, multiple diverging inspection methods are sometimes necessary to address the needs of the case. (*See* ECF 211-5, §§ 8(c)-(d) (providing for source code productions both through a third party neutral and through standalone review computers).)

3. The remaining cases cited by Moog do not support providing proprietary source code to a neutral third party in a trade secret case.

In addition to Moog's inappropriate reliance on *AMO*, Moog's remaining citations do not support its contention that trade secret cases require turning over each side's proprietary source code to a neutral third party for side-by-side inspection.

First, Moog's reliance on *Brocade* is misplaced. *Brocade*, like *AMO*, involves producing source code related to copyright claims. But *Brocade* is instructive, because there, the Court fashioned a protective order with two separate source code provisions: one that allows for side-by-side comparisons (as Moog claims it needs), and a second that allows for source code to be produced on standalone computers (consistent with Skyryse's proposal). (ECF 211-5, §§ 8(c)-(d).) The Court's case management order is clear which of the two protocols applies to which asserted claims. Ex. C (*Brocade Communications Systems, Inc. v. A10 Networks*, C.A. No. 10-cv-03428, Dkt. #90 (N.D. Cal. May 9, 2011). Only "[f]or purposes of the *Copyright claim*" will the parties "be permitted to perform source code comparisons" "at a mutually agreeable third party location." Ex. C ¶ 3. Then, "all subsequent source code review," i.e., the source code review for the trade secret and patent claims and defenses, "will take place at the offices of outside counsel for the party producing source code." Ex. C ¶ 4. The court in *Brocade* was clear: a side-by-side analysis is only necessary and proper for copyright claims, while for trade secret and patent claims, standard source code review on standalone computers is appropriate.

Second, *SMH* also does not bear on the issues currently before the Court. While the protective order in that case did provide that source code should be delivered to a third-party escrow agent, the protective order does not contemplate or provide any means for a side-by-side comparison as Moog is now requesting. (ECF 211-4 § 11.h.) Instead, the protective order merely contemplates that the third party would make the source code available for inspection to the opposing party, as well as making all source code available to a "Court-appointed special master" who would be "appointed by the Court to evaluate source code." (*Id.* §§ 11.g-h.) Here, neither party has contemplated the use of a special master for reviewing source code.

LATHAM & WATKINS LLP

Third, Moog incorrectly relies on *Capstone*, which like *AMO* and *Brocade*, implicates copyright claims, that often do require side-by-side comparisons of source code. *Capstone Logistics Holdings, Inc. v. Navarrete*, C.A. No. 17-cv-4819 (S.D.N.Y.). Additionally, the dispute in *Capstone* was whether source code needed to be produced at all, not the specific protocol by which it would be produced. (ECF 211-1.) Finding that source code did need to be produced, the Court ordered that source code be produced directly from one party to the other, not through a neutral third party. (*Id*.) Here, Skyryse does not dispute whether source code should be discovered, but rather how it will be securely inspected. Nothing in *Capstone* suggests that source code productions should involve remote hosting through a third party, as Moog argues here.

4. Conclusion

Moog requested this supplemental briefing to try pointing the Court to trade secret cases in which the parties' source code is provided to a third party to enable side-by-side comparisons. Moog has failed to do so. Skyryse therefore respectfully requests the Court grant its motion to enter its proposed source code protocol (ECF 213.)

Sincerely,

Gabriel S. Gross
of LATHAM & WATKINS LLP

cc: All counsel of record (via ECF)